Break down siloes to reduce risk faster.

Your challenge:

Siloed teams slow resolution times

In addition to increasing complexity and a larger attack surface, you must also address the sheer velocity with which new workload instances are being spun up. Some organizations are adding hundreds—or even thousands—of new instances overnight, all of which must be protected. Meanwhile, bad actors are using automation to engage in ever more rapid and sophisticated attacks.

Everything is happening much faster—but what about your response? Delays in identifying and patching critical vulnerabilities only increase your risk. Unfortunately, siloed security and IT teams lengthen the delays further. Stitching together tools on your own consumes valuable resources while limiting network access to protect workloads brings its own drawbacks.

Often your people are preoccupied tracking down false positives, which leaves precious little time to respond to the real dangers. And when there is a genuine attack, lack of data and challenges in coordinating your efforts across teams result in longer investigation times and more difficult remediation. With the amount of damage done by an attacker directly proportional to their dwell time, any delay in response is cause for concern. And for business-critical workloads, there is very little tolerance for taking systems offline to resolve a situation. You must get faster in all aspects of protecting your workloads or risk falling behind the pace of the business and leaving security gaps unchecked.

83% of organizations say that their IT and Security teams do not collaborate.

Security As a Team Sport, A Forrester Consulting Thought Leadership Study Commissioned by VMware, May 2020

Your solution:

Break down siloes to reduce risk faster

You're always pressed for time. With VMware, you will simultaneously share the same information with both the security and infrastructure teams, enabling easier collaboration to resolve issues and incidents more quickly. And you will provide both teams with better intelligence by collecting infrastructure and security data comprehensively then providing it to people so that they have all the information needed to take effective action. Finally, you will automate much of the risk and response analysis process, ensuring all issues are evaluated against the same rubric. When you break down siloes and act as a single unit, your people can move with speed and accuracy, reducing vulnerabilities and the impact of attacks to a bare minimum.

Here's how

Put real-time vulnerability and configuration information in the hands of the infrastructure team

To act fast, security and IT need to be working off the same facts. With VMware you can deliver shared visibility. By doing so, you reduce the back-and-forth communication and friction between security and infrastructure—with less lost in translation and less finger-pointing. You build confidence and enable greater collaboration in the process. Your infrastructure team can often proactively patch the most critical gaps before they become a fire drill for security. At the same time, your security staff will gain a better inventory of the highest-priority systems with more in-depth visibility into your workloads. They can decide what needs the greatest protection and where to act first when there is an issue—with less risk of making a mistake because IT is also involved. You enable security and IT to work together as a single team, reducing your attack surface more quickly while responding to incidents before they magnify into a crisis.

The VMware difference: Risk analytics integration

Ability to deliver the same information to both infrastructure and security teams in their respective consoles

Empower Security and IT teams to respond to threats and remediate vulnerabilities with the right context

Your people need a full picture if they are to act with speed and confidence. When you partner with VMware, you will provide your people with full visibility into workload activity. With one platform that contains the relevant data, your teams can easily pivot between contextual information sources to gain the knowledge needed to respond during an incident—understanding the root cause as well as the impact of any remediation efforts.

The VMware difference: detection and response capabilities

Ability to collect and analyze complete data while performing remote remediations from a single platform

Enable IT & Security to talk in the same language

Typically, infrastructure tools are separate and unaware of security issues, particularly in the case of workloads that are ephemeral in nature. But with VMware, you can provide security functionality within the familiarity of the vSphere Client Console so IT can readily address security concerns. With near real-time workload visibility shared by both the security and IT teams, your people will have the information in context they need to drive action. They will be able to protect your workloads across any environment and create self-healing solutions. And because security and IT are always working with the same up-to-date information, things won't get lost in translation when an incident occurs, achieving better resolution quicker. With the information they need now available to them, your people can establish and maintain better-protected, more resilient workloads.

The VMware difference: Built-in security value for IT team

Ability to enable the infrastructure to actively participate in securing workloads

When you **break down siloes**, you will improve your risk analysis integration, expand detection and response capabilities, and achieve built-in security value for your IT team.

With VMware you'll:

- **Enable security and IT to work together as a single team**
- **Respond faster and more accurately to minimize the impact of a breach and avert future attacks**
- **Equip your people to establish and maintain better-protected, more resilient workloads**

To learn more, please visit **vmware.com**